



SPYWOLF

Security Audit Report



Completed on
August 17, 2022

MADE IN USA 

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **Seven22** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08
Good Practices	09
Tokenomics	10
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15



SEVEN22

An abstract, high-contrast black and white image featuring a dynamic splash or ink blot. The black ink forms intricate, swirling patterns against a white background, creating a sense of movement and depth. The text 'SEVEN22' is overlaid in a large, white, outlined font.

SEVEN22

PROJECT DESCRIPTION

According to their website:

The Seven22 Project takes us on a compelling journey through digital artwork to explore and showcase the cultural contributions made by Africans and African-Americans globally.

Release Date: Presale starts on August 22, 2022

Category: NFT



CONTRACT INFO

Token Name

Assigned at deployment

Symbol

Assigned at deployment

Contract Address

Not deployed

Network

Not deployed

Language

Solidity

Deployment Date

Not deployed

Verified?

Yes

Total Supply

Not deployed

Status

Not deployed

TAXES

Buy Tax
none

Sell Tax
none

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of August 17, 2022)



Liquidity

Not added yet



Burn

No burnt tokens

Status:
Not Deployed!

NFT per address
Assigned at
deployment

Additional
information

LP Address(es)

Liquidity not added yet

Team allocation:
Assigned at deployment

Presale price:
Assigned at deployment

Public sale price:
Assigned at deployment



TOKEN TRANSFERS STATS

Transfer Count	Not deployed
Uniq Senders	Not deployed
Uniq Receivers	Not deployed
Total Amount	Not deployed
Median Transfer Amount	Not deployed
Average Transfer Amount	Not deployed
First transfer date	Not deployed
Last transfer date	Not deployed
Days token transferred	Not deployed

SMART CONTRACT STATS

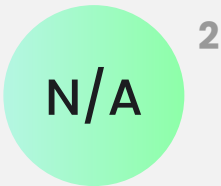
Calls Count	Not deployed
External calls	Not deployed
Internal calls	Not deployed
Transactions count	Not deployed
Uniq Callers	Not deployed
Days contract called	Not deployed
Last transaction time	Not deployed
Created	Not deployed
Create TX	Not deployed
Creator	Not deployed



FEATURED WALLETS

Owner address	Assigned at deployment
Treasury	Assigned at deployment
LP address	Liquidity not added yet

TOP 3 UNLOCKED WALLETS





VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

High Risk

No high risk-level threats found in this contract.

Medium Risk

No Medium risk-level threats found in this contract.

Low Risk

No Low risk-level threats found in this contract.



Informational

Owner can pause contract, making NFT minting impossible.

```
function pause() external onlyOwner {  
    _pause();  
}
```

Owner can change fees.

```
function setFee(uint256 _fee) external onlyOwner {  
    fee = _fee;  
}
```

Owner can set NFT's URI (image).

```
function setBaseURI(string memory _baseUri) external onlyOwner {  
    baseURI = _baseUri;  
  
    emit BaseURI(_baseUri);  
}
```

Owner can withdraw any tokens form the contract.

```
function withdrawTokens(address token, uint256 amount) external onlyOwner {  
    IERC20(token).safeTransfer(_msgSender(), amount);  
}
```

Owner can change price per NFT mint.

```
function setPrices(uint256 _presalePrice, uint256 _publicPrice) external onlyOwner {  
    preSalePrice = _presalePrice;  
    publicPrice = _publicPrice;  
}
```



Informational

Owner can set keyHash.

```
function setKeyHash(bytes32 _keyHash) external onlyOwner {  
    keyHash = _keyHash;  
}
```

Owner can set mintDrop address.

```
function setMintDrop(address _mintDrop) external onlyOwner {  
    mintDrop = _mintDrop;  
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

Seven22

GOOD PRACTICES FOUND

- ✓ The owner cannot set a transaction limit



According to their website:

500 NFT will be reserved for
the pre-sale at price

Price: 0.4279 ETH per NFT

All the remaining assets not
sold in pre-sale + 6,522

Price: 0.8091 ETH per NFT

! There is no information about team allocation in their website
and/or social media pages.

TOKENOMICS



THE TEAM

! The team is
anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL
<https://seven22.io>

Domain Registry
<https://www.godaddy.com>

Domain Expiration
May 3, 2025

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page, appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Blueprint
Well written but a bit short

Roadmap
No

Mobile-friendly?
Yes



seven22.io

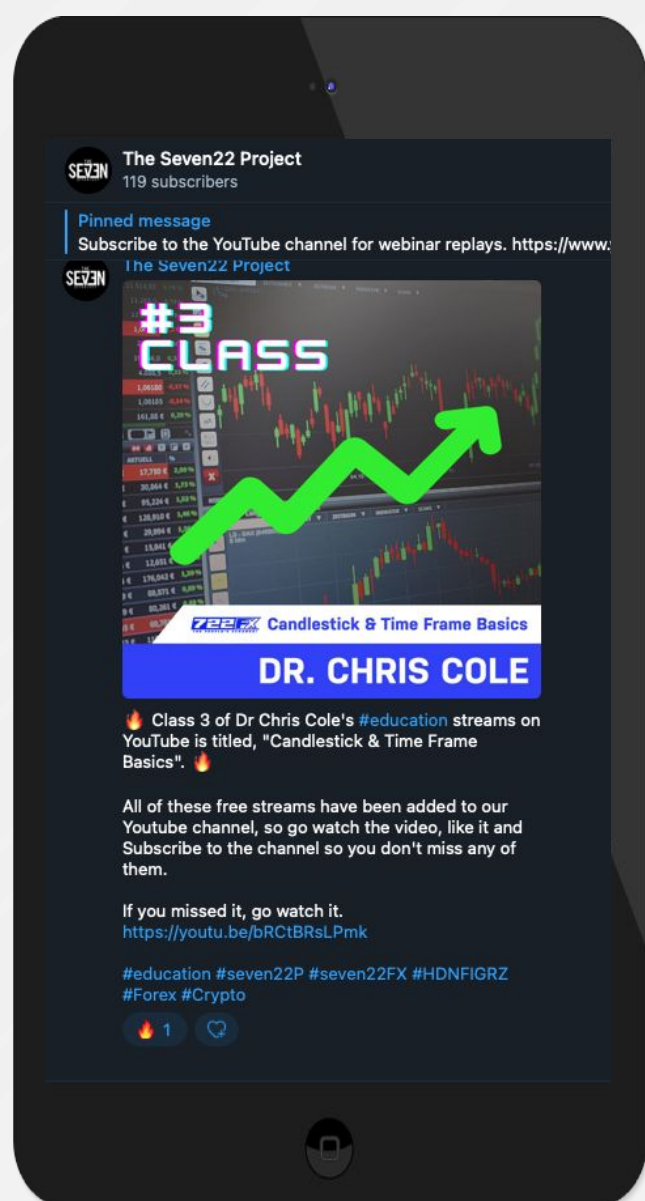


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

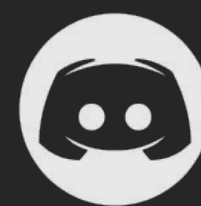
Project's social media pages are active with frequent posts and updates to community



Twitter

@Seven22P

- 12 700 followers
- Very active
- Posts frequently



Discord

- Not available



Telegram

https://t.me/+NvY5l_IL9wtkZGI5

- 118 members
- Announcement channel
- Active



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



SPYWOLF.CO



SPYWOLF.NETWORK



@SPYWOLFNETWORK



@SPYWOLFOFFICIAL



@SPYWOLFNETWORK



@SPYWOLFNETWORK



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.